

ADATBIZTONSÁG KZH FELADATOK

2010. március 16.

1. Az üzenetek halmaza $M = \{a, b\}$, ahol $P(a)=1/3$, $P(b)=2/3$. A kulcsok halmaza $K = \{k1, k2, k3\}$, ahol $P(k1)=1/3$, $P(k2)=1/2$, $P(k3)=1/6$. A rejtett szövegek halmaza $C = \{1, 2, 3\}$. A rejtjelező kódolás:

	a	b
k1	1	3
k2	2	1
k3	3	2

a.) Tökéletes-e a rejtjelező?

b.) A kulcsok feletti eloszlás módosításával változtatható-e az előző kérdésre adható válasz?

2. CRHF tulajdonságúak-e az alábbi kriptográfiai hash függvény jelöltek:

a.) $f(x)=x^e \text{ mod } pq$ RSA kódoló leképezés?

b.) $f(x, y, z)=(x \cdot y) \text{ OR } z \cdot (x+y)$, $|x|=|y|=|z|$, $f: \{0,1\}^{3n} \rightarrow \{0,1\}^n$ (($x \text{ op } y$) bitenként értelmezett AND és XOR) iterációs (kompressziós) függvényre épülő hash függvény, amely DM megerősítést is alkalmaz?

3. Ha mind a titkosság, mind pedig az adatintegritás biztosítása szükséges, egy lehetséges módszer a rejtjelezés és a lenyomatkészítés együttes alkalmazása, az

$E_k(m | H(m))$

kódolás, azaz az üzenetet lenyomattal meghosszabbítjuk, majd rejtjelezünk.

a.) Képezzük a lenyomatot olyan módon, hogy az üzenetblokkokat XOR összeadjuk, továbbá a rejtjelezés legyen CBC módú. Helyes-e a védelemnek ez a módja?

b.) Segít-e az előző problémán az, ha a lenyomatképzést a jól ismert lineáris CRC-vel (Cyclic Redundancy Code) végezzük?

Minden alkérdés 2 pont.

Megfelelt: 2 (6-7p) , 3 (8-9p) , 4 (10-11p) , 5 (12p)

Adatbiztonság KZH megoldások

2010. március 16.

1.

a.) Nem tökéletes. Pl. $P(1/a)=1/3$, de $P(1/b)=1/2$, így nem független a kódoló bemenő és kimenő v.v. .

b.) Igen, lehetséges. Egyenletes a kulcseloszlás esetén tökéletes.

{a.) feladat esetén sokan hibásan próbáltak függetlenséget bizonyítani. Az előadás slide-on kettő rokon feladat látható és kerül előadáson elmagyarázásra}

2.

a.) Nem CRHF. x és x' "lenyomata" azonos, ha $x'=x \bmod pq$

b.) Nem CRHF. Mivel $f(x,y,z)=f(y,x,z)$, ezért nem CRHF a kompressziós függvény.

{a.) feladat esetén – mivel hash függvényről van szó – az x argumentum tetszőleges nemnegatív egész. Ezzel rokon feladat ($f(x)=x^2 \bmod pq$) került előadáson elmondásra.

b.) feladat és megoldása az előadás slide-on is szerepel}

3.

Elegendő, ha ellenőrizhető és elegendő bitméretű redundanciát csatolunk az üzenethez. A CBC rejtjelezett üzenet ugyanis - nagy valószínűséggel - nem módosítható úgy, hogy ne okozzon detektálható változást a dekódolt üzenetben. Tehát

a. Biztonságos.

b. Biztonságos.

{Ha egy integritásvédő kriptográfiai ellenőrzőösszeg lett volna a feladat $[m, E_k(H(m))]$ alakú konstrukcióval, akkor egyik megoldás sem lenne biztonságos. Ezen utóbbi, mint megoldott feladat szerepelt előadáson, míg a fenti 3. feladat technikája az integritásvédő protokollok között a rejtjelezéssel történő védelem alpontban került elmondásra.}